TAB

15 NOV 1982

MEMORANDUM FOR: Chairman, DCI Security Committee

25X1 FROM: [redacted]
CIA Member, DCI Security Committee

SUBJECT: National Policy on Damage Assessments (U)

1. In response to your tasking, the Unauthorized Disclosures Investigations Subcommittee (UDIS) has submitted to me their report, "Points for Consideration Relative to a National Policy on Damage Assessments." The report was unanimously agreed to by all of the UDIS members who attended the 8 October 1982 UDIS meeting (Air Force, Army, CIA, DIA, Energy, FBI, SAFSS, Treasury and Navy). (U)

2. The report points out that a national policy on damage assessments is articulated in Information Security Oversight Office (ISOO) Directive No. 1 (32 CFR Part 2001), and flows from authority granted to the Director of the ISOO in Section 5.2 of Executive Order 12356 (April 6, 1982). The Directive requires that agencies under whose cognizance a loss or possible compromise occurs shall initiate an inquiry to (a) determine the cause, (b) place responsibility, and (c) take corrective measures and appropriate administrative, disciplinary or legal action. (U)

3. There was near unanimity among UDIS members that a full-blown damage assessment would not be appropriate in every case and that inflexible requirements would be counterproductive. If, for example, a safe were left open in a controlled facility and discovered by a security guard soon thereafter, a determination that no materials were missing, and a change of the safe combination should suffice. Despite this general agreement that discretion must be built into the system, there was a division of opinion as to whether there should be national level guidance.

WARNING NOTICE - INTELLIGENCE
SOURCES OR METHODS INVOLVED

[redacted] 25X1

It was suggested that when specialized intelligence equipment or classified military equipment is lost, a human source or a technical collection system is jeopardized, a diplomatic pouch containing classified information is lost, a secure facility is penetrated, or espionage occurs, a full damage assessment should be required unless the Agency head or designee expressly determines that this is not necessary. (This also represents my own position.) (U)

4. Concern was expressed that improved quality control in damage assessments needs to be achieved. At the same time, there was a clear consensus that agencies should not lose control of the damage assessment process. Each agency should conduct its own damage assessment and should be free to structure an investigative framework in accordance with its own realities. Over time, the substantive and technical expertise, along with the security, counterintelligence and audit perspectives represented by participants in damage assessment groups or teams could create or improve upon institutional memory and level of experience in examining compromises. (U)

5. It was suggested that there is little feedback on lessons learned, but it was also recognized that there is a natural concern about airing one's "dirty linen" in public, and justifiable concerns about security, particularly where compartmented or "bigoted" programs are involved. It is felt that a logical military hardware or weapons system grouping exists, and within the Intelligence Community, a distinct SCI Community grouping. Information might be shared within these groups. There has been such sharing at program manager level in the past, but none has been nationally mandated. The Air Force does publish a newsletter (three to four times per year) that synopsizes cases involving unauthorized disclosures of SCI. It was suggested that the Air Force newsletter might serve as a model for others, and that the SECOM might publish such a newsletter for the Intelligence Community. Similarly, the ISOO could publish such a newsletter relating to unauthorized disclosures of collateral classified information. The newly revised DCID 1/19 does already provide for sharing with the SECOM and the DCI summaries of investigations and related actions in cases involving significant compromises. (U)

6. The report suggests the need for an "unauthorized disclosure" database, similar to that established by the Department of Justice and the Federal Bureau of Investigation. There was concern expressed that the information in such a database would be extremely sensitive, but it was suggested that a system might be designed, similar to the 4C System, which would adequately protect the information. While not so stated in the report, it is suggested that such a Government-wide unauthorized disclosure database, as a service of common concern for the Intelligence Community, should operate under the control of the Director of Central Intelligence. (S)

7. The report also notes, as a final point, that agencies which have not yet issued regulations implementing ISOO Directive No. 1 ought to do so. (U)

8. I certainly share the concerns of the UDIS. At CIA, we already have in place mechanisms to conduct damage assessments both internally and at our industrial contractor facilities. Security infractions are investigated and appropriate administrative actions are taken. Punishments range from verbal reprimands through termination from employment, depending on the gravity of the infraction. We have found our Reinvestigation Program and our Agency's use of the polygraph to be exceptionally helpful tools in such matters. More recently, we have drafted a new Agency regulation directed specifically at the conduct of damage assessments. (U)

9. CIA is now heavily involved in security reeducation, both in-house and among our industrial contractor population. I believe that this progam will go a long way toward sensitizing our people to the need for protecting the classified data with which they are entrusted. I would like to see information on the weaknesses of U. S. Government classified information control systems receive judicious dissemination. We can all learn from our mistakes to improve our security posture. Within that context, I consider it useful to pursue development of an unauthorized disclosure database, as suggested by UDIS, provided that proper dissemination controls can be developed and exercised. I would suggest that SECOM is the appropriate forum in which to pursue such an initiative. (U)

[redacted] 25X1